ICANN82 | Fórum da Comunidade – Encontro conjunto: GAC e SSAC
Domingo, 9 de março de 2025 – 16h30 às 17h30 PST

NICOLAS CABALLERO Sejam bem-vindos todos. Por favor, vão ocupando seus lugares. Começa a gravação.

GULTEN TEPE Sejam bem-vindos à reunião do ICANN82, do domingo, dia 9 de março, 16:32, hora local. Essa sessão está sendo gravada e se repetirá esse padrão esperado de comportamento da ICANN e também as políticas de anti-assédio.

Durante a sessão, perguntas e comentários comentadas no chat vão ser lidas em voz alta e na formatação apropriada. Diga seu nome e o idioma no qual vão falar, caso seja diferente a inglês, por favor, falem de forma clara, a uma velocidade razoável para permitir uma interpretação razoável e silenciem seus dispositivos. Podem ter acesso a todas as características disponíveis para esta sessão na barra de ferramentas do Zoom e passo agora a palavra a Nicolas Caballero, quem é presidente do GAC.

NICOLAS CABALLERO Sejam bem-vindos. A última, mas nem por isso menos importante sessão, pelo menos no meu ponto de vista do SSAC, Comitê Assessor de Segurança e Estabilidade. Sejam bem-vindos, RAM, a

equipe fantástica que tem. Estávamos falar sobre das questões, assuntos das quais vamos falar. Ontem falamos e também antes de ontem. E quando eu falei sobre computação quântica, e o impacto no DNS e a estabilidade e sua implementação e também a referida criptografia, todos olharam para mim como se eu fosse um maluco. E pode ser, talvez. Enfim, vamos falar sobre esse assunto com detalhes, com esta equipe de especialistas e também vamos falar sobre computação quântica e sua importância ou impacto na criptografia.

E também vamos falar sobre o estudo Infermal e também o benefício dos novos membros do GAC, eu já expliquei tudo isso, mas vamos falar com detalhes e também sobre o que se está a passar a seguir. Seja bem-vindo Ram e a sua equipe. Passo a palavra para Ram.

RAM MOHAN

Obrigado, Nico. E de parte do SSAC, eu manifesto meu agradecimento ao GAC pelo convite. Esta é a terceira vez que estamos com os senhores e as senhoras e cada vez que estivemos aqui a interação foi muito enriquecedora e há mais participação entre nós. Então valorizamos esta opção para melhorar o diálogo de colaboração com respeito aos assuntos que têm a ver com a segurança e a estabilidade da internet.

Para vocês que são novos aqui no GAC e a comunidade da ICANN, conto muito brevemente que o SSAC serve como organismo de especialistas que assessora a ICANN e quem faz e analisa

potenciais ameaças sobre esses temas de nomes e endereço de internet. Está composta de especialistas e técnicos e oferecemos recomendação com base nas evidências a comunidade da ICANN e a diretoria.

Há momentos nas quais nós não fazemos recomendações com base em evidências e tentamos demonstrar que são opiniões de especialistas que apresentamos à comunidade e à diretoria. Nós trabalhamos com um grande leque sobre a durabilidade do DNS, risco de cibersegurança e também o impacto na infraestrutura e a segurança e estabilidade e resiliência no que tem a ver com a governança da internet. Mas, fundamentalmente, nossas responsabilidades estão dentro da área de infraestrutura crítica. E aí é onde nós participamos.

Entendemos que o papel vital do GAC apresentando as perspectivas dos governos quanto a governança de internet, junto com outros assuntos, claro. Entendemos que isso permite que o SSAC possa unir os domínios técnicos e de política, e o nosso desejo em continuar esta participação é ter a certeza de que nossas recomendações sejam importantes e que fiquem alinhadas com o interesse público. Esse é o objetivo chave. Queremos compartilhar nossas perspectivas, escutar os comentários e continuar assegurando uma estabilidade e resiliência e segurança da internet.

E isso é o que nos leva a fazer esse trabalho. Por isso, agradecemos a participação com o GAC. Há dois assuntos que queremos falar

com vocês. Russ Housley está aqui à minha direita, Russ tem uma carreira longa e distinta e passou também bastante tempo em reparar sobre a computação quântica e o impacto na criptografia. Aqui está Russ para compartilhar as suas opiniões quanto a este tema.

A nossa intenção não é falar sobre o assunto de forma muito específica, mas pedir que os senhores e senhoras compartilhem conosco as suas ideias e que participem, interajam conosco e não queremos que as nossas apresentações sejam muito técnicas, mesmo que o material na verdade é técnico. Estamos aqui e se falamos de maneira muito técnica, perguntem o que é que estamos querendo dizer. Agora eu passo a palavra para Russ.

RUSS HOUSLEY A computação quântica existiu já faz tempo e o Instituto Nacional de Tecnologia e Normas fez uma grande competição e a solução que se fez é uma solução chamada MSLA, que é um algoritmo de assinatura digital com base na lattice, tem uma estrutura modular, isso não encaixa muito bem e o SNSSEC é muito grande, tem valores de assinatura e se usarmos o DNS em lugar do UDP não funciona.

A boa notícia disso é que temos tempo, porque a maior preocupação que temos com o computador quântico é o que nós chamamos de ataque de (inint) [00:08:34]. A questão é que eu sei muitos segredos e eles são guardados e temos um computador criptografado e podem gravar senhas, consegui-las e divulgá-los e

no DNS não há segredos, então esse não é o problema. A nossa preocupação nesse tema é que temos uma assinatura digital que não pode ser falsificada em tempo quando chega ao ponto de precisar de uma mitigação quanto a existência de um computador quântico.

O segundo slide fala sobre qual é alguma das coisas que talvez possamos fazer para poder utilizar essas assinaturas quânticas. Essa é a pesquisa que está em andamento. O grupo de trabalho do Internet vê ou trata o que é o post-quantum do DNSSEC, elas são resposta a muitas coisas, como blockchain, e assinatura transparente e outras cadeias. E aí eu coloquei vários links no slide.

Um deles fala sobre assinaturas baseadas em hash de estado para o DNSSEC, essas assinaturas poderiam ser utilizadas e são bastante grandes junto com outras técnicas, mas a próxima semana no IETF 122, vamos falar um pouco sobre esse tema, mas não esperem a resposta daqui a um ano, mas é tempo. Então, se tiverem alguma pergunta quanto a isso, não sei se fazer as perguntas agora ou no final? Se sim, estão me dizendo que se há perguntas agora que podem ser respondidas.

NICOLAS CABALLERO Obrigado. Por favor, para o benefício do GAC concreto, o que são as assinaturas digitais?

RUSS HOUSLEY É uma assinatura digital. E no que se baseia o DNSSEC. A ideia é que quando conseguimos uma resposta a consulta, a assinatura digital é anexa a isso e quer dizer que não mudou desde que foi publicada originalmente. É o que fornece a integridade e autenticidade dos dados em si mesmo.

NICOLAS CABALLERO Muito obrigado. Agora está aqui Países Baixos.

MARCO HOGEWONING Obrigado. Eu sou o Marco, dos Países Baixos. Obrigado por essa visão geral breve, mas profunda. Ainda precisamos de tempo para fazer alguma coisa. Eu sei que às vezes pensamos que temos bastante tempo, mas não é assim. É mais breve do que pensamos. Sem entrar em detalhes técnicos. Há algum conselho concreto que possa dar para os governos nesse momento? E o que podemos fazer para nos preparar para que o que talvez seja o momento inevitável, onde vamos ter que mudar o algoritmo do DNSSEC.

RUSS HOUSLEY Bom, para o DNSSEC ainda é muito cedo. Para outros protocolos de segurança sim temos soluções, trabalhamos em outros grupos de trabalho de IETF como LAMPS que está trabalhando no PTKI. Temos o TLS e temos IPSEC. Nessas quatro áreas temos soluções onde a infraestrutura deve ser utilizada nesse momento para que quando precisarmos esteja presente, porque vai demorar um tempo.

Se refletirmos quando aconteceu a transição de SHA-1 A SHA-256 e agora o diretório da área de segurança. Bom, eu pensava que cinco anos ia ser suficiente tempo, mas levou o dobro do tempo. Então, comecem com a infraestrutura para que a transição aconteça. Não pode acontecer muitas outras coisas depois, se não existe uma infraestrutura para começar. Essa é o meu conselho.

NICOLAS CABALLERO Steve?

STEVE CROCKER Russ, acho que seria bom fazer um seguimento dessa pergunta, que tem muito sentido quanto ao que podem fazer os governos, falou sobre a transição de SHA-1 a SHA-256. Pode dizer como vai se ver essa transição quando aconteça a decisão de como vai ser esse novo algoritmo ou se mudar esse algoritmo, vai ser diferente comparando com o que já tivemos ou teremos ou é uma mudança no algoritmo onde já temos a prática da experiência?

RUSS HOUSLEY Obrigado, Steve. Não sabemos com certeza essa é a resposta, mas o que sim sabemos é que dessa vez é mais complicado porque não estamos simplesmente mudando uma peça de uma caixa, mas estamos mudando a caixa totalmente. Então, nessa situação se deve ver desse jeito. Se estamos falando de um PKI, estamos falando de construir um desde a raiz, não só mudar as peças, mas totalmente. Não sei se isso ajudou e se não, bom, me desculpem.

NICOLAS CABALLERO Obrigado Steve pela pergunta. Obrigado Russ. Alguma pergunta ou comentário? Mas eu tenho pergunta para você, Russ. Então, o governo X tem uma boa implementação de DNSSEC, de MANRS e PKI, qualquer combinação de RSI, IDAS, SHA-256 ou qualquer combinação dessas coisas. E de repente existe um avanço na computação quântica. Me corrija se me engano, mas nesse caso esse governo com a estrutura do DNSSEC vai ser algo automaticamente absoluto. Estou certo no que eu digo?

RUSS HOUSLEY Sim, mas não fica claro quando vai acontecer isso. É muita bibliografia que estamos vendo sobre avanços na quantidade de qubits e computação quântica, mas agora estamos longe de alguma coisa relevante do ponto de vista quântico, essas coisas não são lineares, acontecem avanços aos pulos, aos saltos em diferentes medidas. Então, quando essas coisas ocorrerem, acontecerem, vão acontecer e não podemos agora responder.

Mas tanto o PKI quanto o DNSSEC são muito singulares quanto a que só precisam de integridade. Não há nenhuma questão lá, não há segredos que colher, então temos mais tempo lá, porque não há uma camada de encriptação de registro que nos preocupe.

NICOLAS CABALLERO Então deveríamos estar bem ai uma combinação de MANRS, RPKI e DNSSEC.

RUSS HOUSLEY Sim, mas agora temos mais tempo para resolver esses problemas, porque só incluem dados públicos e temos integridade.

NICOLAS CABALLERO Está Austrália e Países Baixos.

INGRAM NIBLOCK Sei que cumpre com diferentes propósitos, mas pode falar sobre o papel do DNS sobre HTTPS e DNS HTTP. Podemos passar aos novos algoritmos o tema de segurança, transporte. Vamos ter os benefícios que estamos obtendo agora com o DNSSEC? Através dessa camada de transporte criptografada?

RUSS HOUSLEY Sim e não. Sim vão proteger o tráfego entre o ponto de encriptação e o de desencriptação. É um sistema que vai hop-a-hop, então isso vai nos oferecer proteção. E como eu disse, o trabalho sobre TLS está em andamento. Ainda não temos o PKI para integrá-la. Mas com o navegador, teremos resultados depois da semana que terá lugar em Tóquio com o grupo de Engenharia da Internet.

NICOLAS CABALLERO Obrigado Austrália. Obrigado, Russ. Pelo bem dos novos membros do GAC, quero dizer que PKI é a infraestrutura de chave pública e

MANRS é normas de roteamento acordadas. Tenho Países Baixos e depois aquele senhor, não sei o nome seu. Primeiro Países Baixos.

MARCO HOGEWONING: Obrigado, presidente. Se nós damos um passo lateral, estou evitando que se seja um debate técnico demais, mas no slide anterior, mencionou desafios que temos com o transporte de UDP e lembro que essa não é a primeira vez na indústria do DNS que nos encontramos com limites quanto a UDP como transporte. Acho que também esses se apresentem na implementação atual. Com relação a implementação de DNSSEC, considerando que estamos vendo um horizonte de longo prazo, seria possível considerar diferentes opções de transporte para o DNS para além de UDP?

RUSS HOUSLEY: Quanto as opções de transporte são opções que conhecemos, estão especificadas, mas simplesmente não estão implementadas. Então, como parte dessa transição, talvez sim seja implementado.

MARCO HOGEWONING: E volto a fazer a pergunta. Nós, os governos, como podemos ajudar?

RUSS HOUSLEY: Boa pergunta.

NICOLAS CABALLERO Pode dar dois ou três exemplos de como substituir o UDP?

RUSS HOUSLEY DNS sobre TCP. Esses são exemplos que não têm as mesmas limitações por mensagem.

NICOLAS CABALLERO Obrigado. Países Baixos tem a palavra.

PETER THOMASSEN Fala Peter Thomassen, membro do SSAC. Acho que uma das coisas que foram ditas, podem ser ditas de forma menos técnica e o que está tentando fazer Russ, disse antes que as assinaturas estão anexas a resposta do DNS, e garantem ou são testemunho de que a informação do DNS não se modificou desde que foi publicado. É claro que se todos pudessem anexar uma assinatura, isso seria muito útil.

Então, para anexar uma assinatura de controle de uma chave privada. Por isso é que precisamos de uma assinatura. Então, a computação quântica está tentando falsificar essa assinatura. Também temos o encriptamento, são dados legíveis. Isso também é uma aplicação de chaves. A computação quântica é uma ameaça para as duas aplicações, tanto nas assinaturas computacionais quanto criptografado e descriptografado.

E o DNS não se ocupa disso, mas se preocupa em verificar o momento em que a gente tenta se conectar e fazer uma consulta

ao DNS para verificar que essa assinatura seja válida. Se pessoa quer então trabalhar a respeito isso deveria ser feito em tempo real. Mas se a pessoa consegue registrar, criptografar informação, como a transferência em HTTPS como no passado, podemos passar cinco anos para descriptografar.

Se temos um computador quântico lento, podemos trabalhar com os dados criptografados, mas não seria uma ameaça para a informação do DNS, porque leva cinco anos a acessar. Então aí ninguém vai estar interessado nessa informação, porque de certa forma pode acontecer em segundos. Então a mensagem é com respeito a o que poderiam fazer os governos que fez, por exemplo, Países Baixos.

Com respeito ao DNS, não tenham medo. Por enquanto, é um processo de pesquisa, talvez o problema mais imediato é proteger os dados secretos, armazenados ou em trânsito e o mesmo problema da extração da senha e estão sendo feitos mais avanços com o DNSSEC, queria mencionar apenas isso.

RUSS HOUSLEY Muito obrigado por dirigir a sessão na semana que vem.

RAM MOHAN Nico, quero oferecer ao senhor e ao GAC o seguinte. Se há alguém que tem um projeto inicial nesta área, por favor, entre em contato conosco e vamos poder passar algum material que talvez poderia ser de utilidade. Quando os senhores e senhoras trabalhem com

seus governos, porque aqui há uma diferenciação útil para entender e transmitir a outras pessoas nos seus governos qual é a parte negativa da computação quântica e do DNSSEC com respeito a computação quântica e os segredos compartilhados.

NICOLAS CABALLERO Obrigado, Ram. E muito obrigado, Russ. Eu não tenho totalmente certeza nesse prazo de cinco anos que Peter mencionou, mas obrigado pela explicação. Realmente eu acho que, espero que não, mas eu acho que poderíamos encontrar surpresas no futuro próximo, mas antes de passar a palavra a Jeff, quero saber se há alguma outra pergunta de alguém na sala de forma remota? Vejo que ninguém pede a palavra. Muito obrigado, Russ. Então passaremos agora a Jeff.

JEFF BEDSER Eu sou Jeff Bedser do SSAC. Foi feita uma pergunta para falar sobre o estudo INFERMAL. Esse estudo INFERMAL foi criado pelo escritório do OCTO da ICANN. A área de pesquisa a especialistas, investigadores, pesquisadores que trabalham sobre os domínios maliciosos tentando evitar os phishing.

E uma das primeiras coisas que eu devo advertir e eu coloquei destacada nos outros parágrafos, que não é um relatório que dá soluções, mas resposta às perguntas apresentada pela comunidade. Isso faz com que alguns fatores com respeito onde obtêm os criminosos de cibersegurança, os nomes de domínio

para cometer ataques a incentivos econômicos, verificação proativa, disposições restritas que serviriam para mitigar o uso indevido de seus domínios.

E publicamos um relatório no mês de novembro do ano passado. Passemos ao próximo slide. Quais são os achados chave para aqueles que não leram o relatório? Esta é a parte de incentivos econômicos, uma taxa mais baixa. Cada dólar reduzido corresponde a 49% de aumento no uso malicioso. Também a disponibilidade desse serviço como alojamento web. Isso gerou 88% funções de phishing, no desconto no registro de domínio, teve um grande aumento do registro malicioso. Com respeito às medidas protetivas que podem ser tomadas, há medidas mais restrita quanto a esses domínios, que podem reduzir o mau uso em 63%.

E também há a pequena chance de realizar aquisições de muitos domínios ao mesmo tempo. Isso pode representar 401% de aumento nos domínios maliciosos registrados e práticas de verificação proativa de informação de registratário com endereço de telefone, de correio eletrônico. Isso reduz as registrações maliciosas. Próximo slide.

Quais as medidas de reação, o impacto sobre a redução do uso indevido é mínimo e, inclusive, um breve tempo serve para que os atacantes acedam, tenha acesso a lucros importantes e roubo de dados. Também constituição de uso indevido de registrações maliciosas que são distribuídas de forma uniforme e que se reúnem

alguns registradores de TLD, que eles oferecem também preços baixos e serviços gratuitos.

Está é uma informação que está validada, que já existe entre a comunidade do uso indevido há muito tempo atrás, o tema se chama lucro econômico. Os compradores vão onde podem comprar a um preço menor, onde podem comprar grandes quantidades, são muitos lugares no mundo onde há grandes entidades que vendem grandes quantidades de todo tipo de produtos, e que vendem a um preço menor.

Então, essa é uma leitura legítima dos dados, não significa necessariamente uma resolução do problema, porque se a pessoa aumenta o piso do preço igual, vai existir um preço mais baixo. Considerando as diferentes economias do mundo, as diferentes moedas. E não vamos eliminar aqui o problema desta forma. Também estão as perdas por crime cibernético, números que vão de 1 quadrilhão até 10 quadrilhões. Eu acho que esses são valores possíveis. A diferença 1 e 10 quadrilhões é um número muito alto se falamos de perdas, a maioria dos estudos, a perda média por phishing é de 136 dólares e nos Estados Unidos esse número sobe para 3.520 dólares pelo phishing.

Eu vi variantes de todos esses números e aqueles que trabalham nesta área conhecem muito bem esses números e depende de cada estudo. Então, a realidade é que cada mínimo de perda representa, deve representar no mínimo a 136 dólares. Isso faz com que aqueles que ganham muito dinheiro com crimes não querem

se dedicar a atividades não criminosas. Então, quais as mudanças que podemos reduzir ou mitigar o problema das registro? Uma licença utilizada para cometer crimes cibernéticos, para roubar dinheiro, para prejudicar as pessoas. Se mudarmos o preço, isso vai mudar. Os incentivos dos criminosos para ganhar centenas de milhares de dólares, se o domínio passa de 10 dólares por ano. Eu deixo essa pergunta. Seguinte Slide.

Então o processo de verificação, mais uma vez como já mencionei, esse é o relatório de novembro com dados daquela época no ano passado, a questão de inteligência artificial continua acelerando a um ritmo que supera o ritmo o qual avança a computação quântica. Mas neste momento, a capacidade de criar identidades geradas digitalmente e podemos tomar o nome real de uma pessoa e dizer agora é uma inteligência artificial, eu preciso um registro de conduzir de habilitação com essa formatação, mas com nome de uma pessoa real da mesma idade que tem uma foto parecida a minha ou utilize a minha própria foto para poder gerar digitalmente uma identidade que depois possa utilizar no processo para registrar um domínio.

Isso afeta muito a capacidade de dizer bom, se apenas verificam a identidade do registrador, vão resolver o problema. A chance de diferenciar uma coisa real de falso a partir de uma foto já vamos precisar de inteligência artificial para fazer essa diferenciação, porque os seres humanos não podem fazer. Então, quais os

melhores processo para que os domínios não sejam registrados de forma fraudulenta, fora o que é a verificação manual.

Também existe o problema de determinar, e isso é uma medida válida. A maioria dos estudos feitos utilizam os recursos disponíveis publicamente quanto aos volumes ou quantidade do uso indevido do DNS e são números realmente que provocam choque. Mas o uso indevido do DNS, o phishing, em especial, têm como base as entidades para que tentem reportar.

Os relatórios gerados nesse tema são fixados nessas informações. Quantas vezes você vê um phishing no celular e está dizendo não me pegou, mas quem de vocês reportou esse fato. Se fizeram, eu os elogio, mas acho que nem muitos. Mas se não reportamos essas ações não ficam visíveis para a indústria, para conseguir mitigar, então mudar a metodologia na registração é uma solução possível, mas também há melhores oportunidades de detectar e mitigar de forma imediata esses problemas para que se apareça um domínio por seis ou sete segundos podemos imediatamente remover, mas se demora dois dias, alguém reporta e leva dois dias para validar, então já são quatro dias e o que queremos é detectar assim que possível para remover imediatamente.

Obviamente quanto a outro ponto de medição, uma coisa que já deveríamos estar fazendo, mas ver os números das vítimas por cada domínio, porque podemos ter cem vítima num segundo por um phishing muito bem feito. Então não é necessário o número de domínios que estão o phishing, mas as vítimas que caem nessa

armadilha. Sabemos que estamos falando do topo do iceberg, que é um recurso disponível que fala do phishing. Vemos o volume disso, mas são muitos que nos reportam e não ficam à vista, visíveis. Mas há muita coisa que deveria reportar. Então temos que ver as vítimas para calcular o prejuízo financeiro.

Falo de tudo isso, porque esse relatório INFERMAL valida muito bem que preços mais baixos incentivam todo esse trabalho, preço mais baixo para os registratários incentiva esse phishing. Então como chegamos ao seguinte passo ou etapa, o que podemos fazer para melhorar e medir o impacto da melhor forma e como detectar isso para sermos mais eficazes em deter esse problema?

Porque eu diria que mesmo que cobremos mais 1.000 dólares por domínio por ano, por exemplo, o que estamos fazendo é eliminando a habilidade da pessoa de ter um domínio na internet pelo custo, mas não fazemos nada com os cibercriminosos que ganham ou que vão ter uma margem de lucro muito grande. Então temos que procurar uma solução. Muito obrigado.

NICOLAS CABALLERO

Obrigado, Jeff. Por favor, coloquem o próximo slide. O aumento de 400%, eu adoraria ter essa conversa neste momento e a questão do API, interface de aplicação e programação. Realmente esse é o problema, que os criminosos têm acesso ao API usando a telecinesia artificial ou qualquer coisa assim, são mais capazes de

provocar danos e aumentar as atividades de phishing. Esse seria o caso?

JEFF BEDSER

Não tenho dúvidas de que essa registração é um veículo para grande acesso ao uso indevido. Mas 401% um ator ruim que está registrando esse domínio, algoritmos para botnet pode estar também escrevendo, registrando mil domínios e isso não significa que a API é ruim, porque essa percentagem pode ser comparada com vários (inint) [00:37:48] API.

Por outra parte, se chegasse a haver esse espaço onde alguém registra 50 domínios. Esses domínios que estão se registrando vão ser para fazer alguma coisa ruim? Há muita informação de infraestrutura que serve para saber se vai ser para alguma coisa ruim ou não. E ao mesmo tempo, eu diria que o problema é a falta de restrição.

NICOLAS CABALLERO

Obrigado. Tem alguma pergunta, comentário? Eu não vejo mãos levantadas. Há duas mãos. Está Índia e Austrália, Índia tem a palavra.

SUSHIL PAL

Eu acho que é claro que a verificação é uma questão, é um problema. Se temos credenciais verificadas dos registradores, então o uso indevido do DNS se reduz ou não é tanto assim. Não é

a inteligência artificial o problema, mas as credenciais que não são verificadas e são compartilhadas através dos KPIs.

O problema é claro, mas ainda temos que saber com a GNSO como definir a veracidade dos dados e o âmbito dos dados, porque se não desistimos, o âmbito da veracidade dos dados no WHOIS nunca então poderemos verificá-lo. Então, o GAC ou SSAC talvez possam instar o GNSO a que acelere o processo, porque senão não podemos dar um passo para frente para poder restringir isso.

JEFF BEDSER Algo que acho que não fui claro na minha apresentação é que as pessoas que estão utilizando o domínio para esse propósito, com quem estamos batalhando estão 10 ou 100 passos antes do que nós. Então, a tendência recente é que são pessoas legítimas, com credenciais legítimas. Cria uma conta e através dos meses cria um portfólio de domínios e vendem com essas credenciais a um delinquente que depois utiliza esse domínio para propósitos ruins.

Embora envolva melhor fricção com melhor verificação de credenciais. Mas meu ponto é que se nós baseamos muito isso como uma solução, isso é um problema. A outra preocupação real é que essa é uma sessão pública e eu garanto que as pessoas com quem estamos batalhando já verão isto vão saber sobre essa informação e vão decidir quais os passos a fazer para continuar com a delinquência.

Quando falamos do que podemos fazer, tem a ver com o que vimos no slide anterior, manter melhor detecção, e também na aceleração no processo de mitigação, é a ideia. Não podemos ter um incentivo econômico porque os delinquentes continuam roubando as pessoas apesar disso.

Mas se pudessem não saber como fazê-lo, onde a pessoa faz, pegamos a pessoa e minimizá-lo, pelo menos até certo ponto. E se esses incentivos já não existem. Não sei se estão me entendendo, mas o ponto é que se deve buscar a melhor detecção e melhores taxas de mitigação. É o que vai ajudar esses problemas.

SUSHIL PAL

Quando falamos da verificação, não estou dizendo que essa seja a solução completa, mas é um passo a dar. Eu sei que estamos falando e falando nisso, mas não estamos dando um passo para frente quanto a verificação. No ccTLDs, onde operamos, por exemplo, no nosso país, temos um processo de verificação de dois passos e significativamente se reduziu esses usos indevidos.

Mas é um grande custo que temos devido a esses ciberataques. É importante para nós reconhecer que o primeiro passo deve ser tomado e não queremos menosprezar a importância da detecção e adquirir capacidade para monitorizar isto.

NICOLAS CABALLERO

Obrigado, Índia. Tem Austrália, Comissão Europeia, Reino Unido e Países Baixos. Vamos continuar com a Austrália.

INGRAM NIBLOCK

Quais os passos quanto a pesquisa do estudo INFERMAL. Estamos vendo as características dos registradores, mas há alguma forma de validar essa hipótese com os registradores? Porque temos domínios em particular que têm em sua lista de bloqueio e utilizam na sua pesquisa, mas em escala, conseguir dados utilizáveis quanto ao que estão fazendo essas pessoas nessas instâncias e o uso indevido. E que dados têm supostamente o registrador? Esses seriam passos a tomar na pesquisa em si.

JEFF BEDSER

Sim, teria que referi-lo ao escritório do OCTO quanto a seus relatórios e passos a tomar. O que poderia dizer aqui talvez não é uma resposta apropriada do que estou dizendo.

NICOLAS CABALLERO

Obrigado, Austrália. Agora a Comissão Europeia.

GEMMA CAROLILLO

Minha colega Martina já falou sobre o uso indevido do DNS no chat. Então vamos ter uma apresentação do relatório na sessão de uso indevido do DNS e também com a intervenção de OCTO. Então vou deixar que eles façam a pergunta.

Uma é uma pergunta geral que eu tenho como esse relatório de INFERMAL tem muito eco e escutamos os seus comentários em certos aspectos. Vocês têm alguma declaração com relação aos

comentários do relatório que possamos acessar relativos ao uso indevido do DNS e aspectos do relatório, porque vai nos ajudar a ler o documento. Segunda pergunta. Entendo que o problema não é API, mas como a registração é o problema, quem devemos entender que deve existir restrições quanto ao uso do API ou talvez tratar o tema do que tem a ver com as registrações.

JEFF BEDSER

Isso não vem de um documento de SSAC. Esse documento vem do SSAC. Um consenso podemos conseguir com relação ao relatório de INFERMAL. A segunda pergunta eu esqueci. Desculpe. Bem, quanto aos dados de registração massivos ou maciços, acho que há uma corporação que está estabelecendo uma nova marca ou identidade e tem que registrar essa entidade através de vários TLDs, e esses podem ser mil registros nesse momento.

Essa ferramenta tem um propósito válido nessa instância, mas é difícil para mim uma quantidade mais alta onde possa ser o caso e o que tem a ver com essas registraçoes maciças. Mas geralmente há regras para conseguir, por exemplo, uma licença para dirigir uma moto ou carro e diferentes para um caminhão.

Devemos conseguir diferentes licenças devido a habilidade necessária para não lesar as pessoas ou feri-las. E eu uso esse exemplo para mostrar que a ferramenta de API é similar ao exemplo que eu coloquei de um caminhão onde a gente precisa

passar por um processo mais rigoroso. Então não é a ferramenta, mas a licença que se dá para utilizar essa ferramenta.

NICOLAS CABALLERO Tem a palavra Reino Unido.

NIGEL HICKSON Isso foi extremamente interessante. Com esse relatório importante em contexto e que O SSAC a análise. Quero agradecê-lo. E eu me perguntava se isto poderia continuar e talvez se transformar numa recomendação, considerando a importância das recomendações que vocês publicam ocasionalmente. Obrigado.

RAM MOHAN Obrigado, Nigel. Não chegamos ainda ao ponto em que definimos ou decidimos se temos que fazer uma recomendação ao respeito. O escritório de OCTO fez uma apresentação diante da SSAC sobre esse assunto também. Mas o que não fizemos foi olhar e dizer há algo a mais, algo por cima. Em parte, se deve ao fato de que parte do trabalho que se faz aqui, é mais sobre desenvolvimento de políticas da ICANN e não de assessoramento técnico.

O relatório INFERMAL deu bastante assessoramento técnico, mas isso é o que eu penso. Embora não tenhamos tido uma discussão específica sobre SSAC sobre esse tema. Obrigado pela sugestão. Vamos colocá-lo quando tivermos a próxima conversa dentro do SSAC para ver o que opinam os membros do SSAC.

NICOLAS CABALLERO Obrigado. Agora fala o representante de Países Baixos.

MARCO HOGEWONING Em termos de pesquisa, esse é um problema de política. E Jeff falou sobre melhorar a detecção e a API. E eu me pergunto se fora das discussões sobre políticas, teríamos que falar acerca dos padrões técnicos que poderiam melhorar para melhorar a detecção e esse seja parte do problema. Há espaço para soluções técnicas?

RAM MOHAN Vou falar brevemente, talvez Jeff possa adicionar. Não sei se há uma solução técnica necessariamente, mas é um componente de educação. Quando a gente recebe um phishing ou smashed sabemos o que fazer, não apenas como detectá-lo, mas também como informar, denunciá-lo.

Um dos problemas que temos dentro da comunidade é que não se denuncia, então não podemos coletar os dados suficientes como para poder dizer houve 1000 casos informados, 10%. São casos aos que não se respondeu de forma determinada. E vejamos esses 10%, ou seja, qual for o percentual, ver quem está por trás disso e ver quais os padrões para tentar entender quais as condutas, características dentro do ecossistema.

Então, algo prático seria levar a cabo uma campanha de educação sólida, que diga, denuncia o uso indevido, denuncia o phishing, denuncia essas coisas. Então, depois de fazer isto, podemos fazer

um seguimento do que se fez. Depois poderemos contar com dados que nos darão um foco real do problema e de onde poderia estar o problema e o que poderia estar contribuindo para o problema.

Pelo momento, estamos no modo no qual com frequência tentamos aplicar uma abordagem geral e dizemos que criemos uma política que se possa aplicar a todos. Então se identifiquemos um grupo de diretores determinado quando há atores dentro que fazem um trabalho excelente e outros fazem um trabalho muito ruim, então o foco deveria estar naqueles que não chegam ao nível adequado.

Agora que temos os dados podemos falar, essas são as normas, as exigências e os requisitos que devemos cumprir. Acho que as melhores práticas podem se concretizar ou criar sem desenvolvimento de políticas, porque estamos dizendo, olha, essa coisa é boa para ter um ecossistema mais saudável, mais sadio.

NICOLAS CABALLERO Obrigado, Ram. Eu vejo que a República Dominicana pediu a palavra.

AMPARO ARANGO É um painel muito importante. Muito técnico, mas acho que está no coração do que estamos enfrentando hoje em dia com nossos países. Eu quero falar como governo e como um país pequeno, República Dominicana, e o senhor já no final estava dizendo o que

devemos fazer nós como governo. Primeiro saber qual a situação nos nossos países, nos nossos próprios administradores de domínio, operadores.

Eu sou da entidade de telecomunicações, nossos operadores, o nosso centro de cibersegurança, centro de resposta aos ataques, porque tivemos nos últimos anos. Costa Rica no passado, passou dois anos numa situação terrível que custou milhões e milhões de pesos, atacaram todos os sistemas de saúde e nós tivemos outras coisas semelhantes.

Enfim, desde nossa perspectiva como governo e talvez os senhor não podem falar tão claramente, mas eu acho que precisamos estratégias, orientações mais claras de como promover isto que tem a ver com DNSSEC nos nossos países, quantos atores conhecem o DNSSEC, quem não conhece, os nossos operadores de segurança, administradores de domínio. Eu não sei se no meu país tem ou não tem, mas por aí está a chave de como atacar esse problema de cibersegurança e de insegurança que temos tão grande.

Então, eu gostaria de escutar como recomendações, mas eu acho que isso vai ser entre o SSAC e com o GAC, porque no final das contas nós temos que tornar ferramentas específicas para poder trabalhar, regulação, educação leva um custo alto, ter uma estratégia nacional onde todos os sistemas tenham DNSSEC. Enfim, estou fazendo uma reflexão, não sei se podem responder,

mas enfim, me angustia tudo isso. Eu acho que temos ferramentas para pelo menos mitigar esses impactos. Obrigado.

RAM MOHAN

Obrigada pelo comentário. Uma resposta muito importante são os desafios e os desafios do SSAC, que podemos oferecer muitos conhecimentos técnicos e informação técnica. Mas o que não entendemos totalmente bem e o que não temos é saber quais são as suas necessidades. Que nível de informação precisam, então temos que colaborar para compreender os atuais que tipos de informação querem que nós ofereçamos.

Uma coisa que podemos fazer é antes fazíamos o trabalho e publicávamos relatórios muito técnicos que podiam ir de 10 páginas até 40 páginas de extensão. Uma das coisas que começamos a fazer é tornar esse relatório em resumos de 500 ou 1000 palavras que possam prestar como resumos executivos ou briefings do que tentamos falar através desse relatório. Mas continua isso centrando, no trabalho da nossa série de investigação pesquisa do que nós pensamos que é importante.

Convidamos os senhores e senhoras a que falem conosco. Adoraríamos trabalhar de forma direta com vocês, mas o GAC pode falar, olha, trabalhem juntos para dar para a gente clareza quanto a duas coisas por uma parte a classe de informação que precisam e também o nível de informação que precisam, os detalhes técnicos que querem, porque nós começamos de forma predeterminada, com o nível técnico muito elevado, muito

profundo, porque está bem, engenharia é a nossa especialidade, mas se vocês quiserem que a gente levante o nível, também podemos entrar em contato, trabalhando em conjunto.

NICOLAS CABALLERO

Alguém tem a mão levantada ali? Ficou de antes? Temos que ir encerrando. Temos apenas um minuto. Pergunta ou comentário final por parte do GAC? Fala o representante do Japão.

NÃO IDENTIFICADO

Obrigado pela apresentação. O senhor destacou a importância dos dados. Eu acho que há diferentes usos indevidos do DNS, não só a definição da ICANN, mas também há outras formas de uso indevido e outro tipo de violação de dados que se produzem no Japão e em outras áreas também. Eu acho que o problema inicial é o mesmo e quero saber se é necessário reunir diferentes tipos de dados sobre o uso indevido e se trabalhamos assim, talvez poderíamos colaborar com os diferentes governos para obter essa informação.

RAM MOHAN

Acho que é um tema importante. E nós estamos preparados para trabalhar junto com vocês para passar essa informação técnica e as recomendações técnicas que precisem. Então, a solução potencial seja talvez uma combinação da parte do governo, a parte técnica e de políticas também. E temos que encontrar uma forma de integrar tudo isso dentro deste fórum.

NICOLAS CABALLERO	Muito obrigado, Ram. Temos que encerrar a sessão. Obrigado pelas perguntas. Foi mais uma sessão fantástica, Ram. Como sempre é um prazer recebê-los aqui. Estas conversas são um pouco técnicas, tentamos de transmitir a mensagem e vocês fazem todo o possível por dar boas recomendações por uma parte e ajudar a lutar contra os criminosos. Então, mais uma vez, obrigado. Obrigado Russ, tem uma equipe fantástica e esperamos ter outra sessão em Praga. Muito obrigado. Uma salva de palmas para os nossos amigos do SSAC. Muito obrigado. Damos por encerrada a sessão. Vamos começar amanhã 09 horas para a cerimônia de abertura e outorga de prêmio à excelência na comunidade. Muito obrigado e boa tarde.

[FIM DA TRANSCRIÇÃO]